DATE(S) ISSUED:

08/12/2014

SUBJECT:

Cumulative Security Update for Internet Explorer (MS14-051)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining elevated privileges on the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

This advisory covers one publicly and twenty-five privately disclosed vulnerabilities. There has not been any active exploitation or exploit code observed for any of these vulnerabilities at the time of their announcement.

SYSTEM AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**
Home users: **High**

TECHNICAL SUMMARY:

Multiple vulnerabilities were discovered in Internet Explorer due to the way objects in memory are improperly accessed. The vulnerabilities are as follows:

- Twenty-four memory corruption vulnerabilities
- Two Elevation of Privilege vulnerabilities

These vulnerabilities could allow an attacker to execute remote code by luring a victim to a malicious website. When the website is visited, the attacker's script will run with same permissions as the affected user account. Successful exploitation of these vulnerabilities could result in an attacker gaining elevated privileges on the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/ms14-051

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2817

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2819

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2774

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2784

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2796

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2808

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2810

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2811

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2818

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2820

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2821

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2822

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2823

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2824

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2825

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2826

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2827

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4050

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4051

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4052

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4055

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4056

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4057

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4058

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4063

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4067